

# Implementing Identity Management with BMC Control-SA


Adrian Grigore

Adrian Grigore
GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b – Option 2
September 22, 2003

**Implementing Identity Management with BMC Control-SA**

# Abstract

Identity Management is a relatively new concept, which aims at solving the issue of centralized access control security administration across multiple platforms and applications. "Identity Management is essentially an infrastructure that encompasses many technologies from user provisioning to authentication and access management."[1]
With centralized security administration, one company could enforce a consistent security policy (such as password policy, user rights, etc) as well as manage user accounts, users groups or other entities across the entire enterprise from a central point.

This paper is a case study describing how the organization I work for implemented Identity Management using BMC Control-SA product. I will present the situation before and after implementing Control-SA and outline the benefits realized from this implementation. There are several products available aimed at providing similar functionality, however this paper is not intended to compare products or provide detailed reasons why this product was chosen over other products.

# Introduction

"Identity is at the core of any business or data transaction. It is a critical component of the operations of any enterprise, and is interwoven into most business processes, including granting access to information and systems, enabling Customer Relationship Management (CRM) systems, and driving relationships with business partners and suppliers."[2]
Companies with large heterogeneous networks face the difficult problem of maintaining tight access control over their systems and applications. Generally there are system administrators for each type of platform (such as RACF, Windows NT, UNIX, etc) and applications (such as Oracle, Microsoft Exchange, Entrust, etc). In many cases the system administrator (i.e. Unix administrator) is

[1] http://www.rsasecurity.com/solutions/idmgt/whitepapers/IDROI_WP_0403.pdf

[2] http://www.projectliberty.org/resources/whitepapers/LAP%20Business%20Benefits%20White%20Paper%20v4.pdf

given the job of the security administrator for that system. Homegrown applications usually rely on their own security mechanism and have non-security personnel, such as the manager of the department using the application, perform security-oriented tasks such as adding, modifying, deleting users, changing passwords, changing permissions. Delegating security administration to other department or individuals (security administrators) in many cases requires that the security administrators be granted elevated privileges such as Accounts Operators in Windows NT or Group Special or Global Special in RACF (this is the equivalent of superuser account in Unix). By default, the Unix security mechanism has only one administrator (root, or the user with a User ID of 0) posing additional challenges when it comes to delegating security administration. There are Unix programs such as "sudo"[3] that allow delegation of administration tasks without giving out the root password or creating additional root accounts. However, if not properly managed, they too contribute to privilege escalation.
It becomes evident that under these circumstances it is hard to implement proper separation of duties and the least privilege principles.
Lack of centralized account management could lead to multiple accounts for a single user, user privileges not being removed when the user moves to a different department and inconsistent ways of creating user accounts.
Employees moving from one department to another represent one of security's biggest challenges, as it requires cooperation between individual business units (i.e. Sales, Marketing, etc.), Human Resources, Security and IT departments. If access rights are not managed appropriately employees could end-up having excessive privileges with negative consequences regarding the confidentiality, integrity and availability of information assets.
Duplicate accounts represent a security risk since they are most of the time forgotten; left inactive they represent points of entry to attackers. Attacks on inactive accounts are likely to go undetected.
Another important aspect of Identity Management is to ensure that when employees leave the company all their user accounts are disabled and eventually deleted. Old user accounts are then not subject to be used by external hackers attempting to gain access, nor are they available for employees to gain un-authorized access or privileges.
Inconsistent methods of creating user accounts could lead to difficulty in spotting rogue accounts, reporting and auditing user access. In other words, this would be an overall administrative nightmare.
"Identity management includes the entire process of deciding who should get what access to which resources; providing, changing and terminating such access when appropriate; managing the process and monitoring it for compliance with internal and external policies." [4]

[3] http://www.courtesan.com/sudo/

[4] http://www.businesslayers.com/site/sol_identity.asp

## Before

The same issues applied to the company I'm working for. When I joined the company, the Information Security department was less than 6 months old and there were only 2 full time employees in the department.
The company uses a problem management ticketing system to keep track of all user requests by assigning tasks to each department or responsible person. Even then, it would take time (sometimes days) to process a new user request, a modify request when an employee moves to a different department or a revoke request when an employee leaves the company.
The Help Desk department was responsible for password resets and account unlock for Windows NT. They could not manage accounts from other platforms, such as mainframe, Unix, Oracle, etc. Help Desk needed the Account Operators user rights in the Windows NT domain to allow management of the accounts; however, they could not manage accounts with equal or higher privileges such as Domain Administrators. These kind of requests had to be passed to the second level support team, System Administration, which was in charge of creation, modification and deletion of user accounts on all the platforms and applications. It was very difficult to obtain a holistic view for the entire enterprise, to report on what resources (as in systems and applications) an employee has access to, or ensure all access is immediately terminated when an employee leaves the organization.

Password management was also a problem. Users were required to remember many passwords for all the systems and applications they had access to. This leads to users selecting weak passwords that are easy to remember and a large number of calls to Help Desk for resetting passwords or unlock accounts.
A study conducted internally indicated that more than 40% of the Help Desk calls were password related.

## During

I work for a heavily regulated company with offices in Canada and the US. Therefore, privacy legislation such as Personal Information Protection and Electronic Data Act (PIPEDA), Graham-Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), amongst others, is applicable. Noticing a lack of logical and technical access control mechanisms in my company, I proposed the implementation of an Identity Management solution that would address these concerns and help meet privacy legislation requirements. Identity Management helps ensure confidentiality, integrity, availability and accountability by promoting proper access control mechanisms and security auditing capabilities. Together with a coworker I put forward the business case with emphasis on both legislative compliance and cost savings for user provisioning.

The Identity Management solution that we were looking for had to meet the following requirements:

- Support a wide range of operating systems and applications including the following: Windows NT 4.0, Windows 2000 (with Active Directory), Unix (Solaris and HP-UX), RACF, Oracle, Entrust CA, LDAP, Exchange 5.5 and Exchange 2000.
- Provide centralized administration of user accounts, groups and other entities (such as User Rights, Audit Policy, etc) for the operating systems mentioned above from a single console.
- Provide detailed audit trails of activities performed using this tool.
- Allow for self-user administration. Users should be able to reset and synchronize their passwords across multiple systems without calling Help Desk or administrators.
- Ability to capture changes to the managed systems and report them to the central console (such as accounts modified using native tools).
- Security. All transactions and communication with the managed systems should be encrypted. Access to the application should be restricted to authorized users and the application should have good granularity for granting access privileges. Allow for delegation of administration functions while maintaining strict control over what administrators can do.
- Flexibility that would allow extending this architecture to in-house built applications.

BMC Control-SA product was selected as it met most of our requirements.

## BMC Control-SA Explained

"Control-SA is an integrated client/server solution consisting of Enterprise Security Station, which is the central point of control, and SA-Agent, which runs on any number of managed platforms or networks throughout your organization. Each instance of SA-Agent interfaces with access control systems or other applications that require user and resource administration. Each such system is referred to as Resident Security System or RSS." [5]

Summary benefits of Control-SA:

- Holistic view of the enterprise. With one click you can see what users have access to what system and the level of access. This is very useful in heterogeneous environments when conducting audits as well as for day-to- day management.
- Supports more than 50 platforms (operating systems) and applications.
- Real-time bi-directional management. This ensures that user and account information in the centralized database is consistent with the target system.
- Intercepting security violations on the target system.

[5] Enterprise SecurityStation User Guide (Windows GUI), Version 3.2.00, December 9, 2001, p 1-3

- Secure communication protocol (3DES). The main application communicates with the remote agents using the 3DES encryption. End-user GUI communicates with the main application using SSL encryption.
- Consolidation of account management logs and reporting. Detailed audit and transaction logs will show all the account management activities performed from Control-SA or using the native tools. Un-authorized activity is easier to spot.
- Pre and post-scripts can be created using native system commands to extend Control-SA capabilities and automate tasks. For instance, when creating an NT user account, the post-script can create the home directory for the user on the required server. When deleting a user account, the pre-script can delete or move all files belonging to the user before the account is deleted.
- Allows users to manage their own accounts in terms of password resets, accounts unlock or even registering new accounts.

The Control-SA architecture as it was implemented in our environment is illustrated in the Figure 1 below:

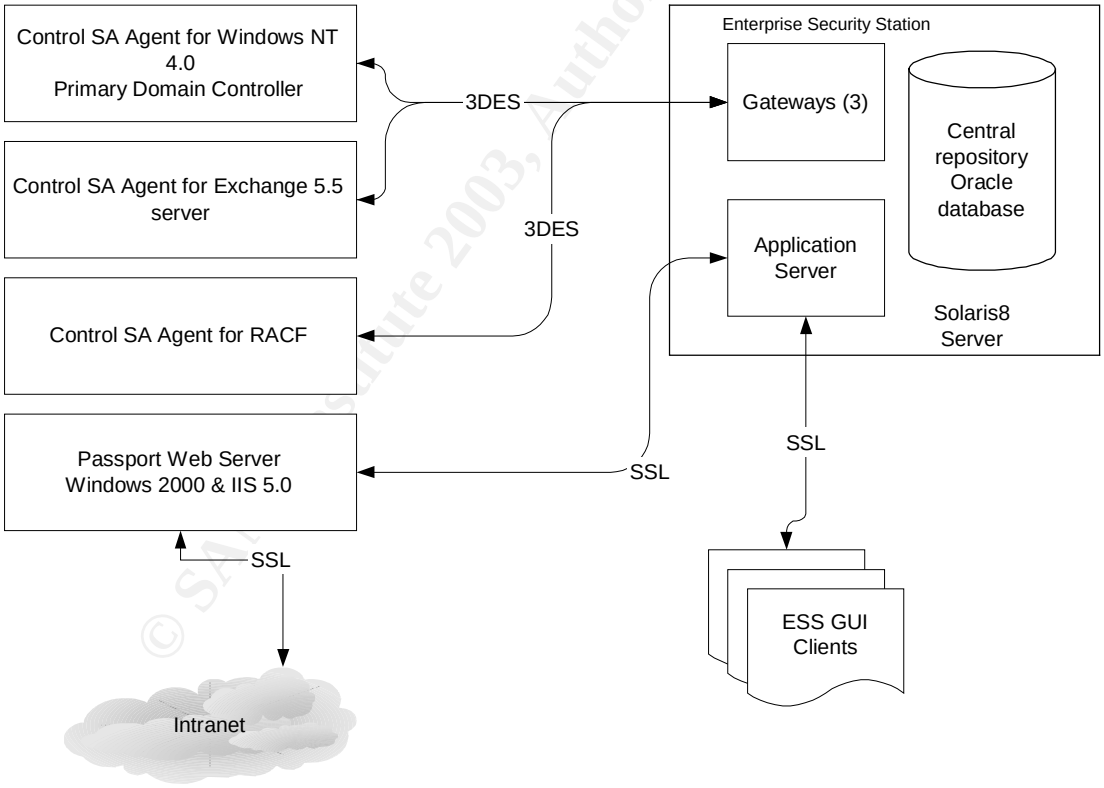


**Figure 1**

Control-SA consists of the Enterprise Security Station (ESS), Control-SA Agents and GUI Clients. ESS is the main application and includes a Sybase or Oracle database. ESS communicates with agents installed on the Resident Security

Systems (RSS) through a gateway using a choice of no encryption, DES or 3DES. The agent's role is to execute instructions received from ESS as well as monitor the RSS for changes that were made using native tools and report them back to ESS to ensure the database is up-to-date. An On-Line and Off-Line Interceptor takes care of this task on the Control-SA agent side. Multiple agents can co-exist on the same system. ESS is accessed using the Control-SA Windows GUI. This is the program used by administrators for managing the RSS (e.g. create/modify/delete accounts, groups, etc) at the enterprise level as well as for reporting and auditing. Control-SA Passport enables users to manage their accounts using a web browser.

## Implementation

BMC Professional Services were contracted for the first phase of implementing Control-SA. I was the technical lead of the project and the application support specialist once implemented.

First we installed Control-SA in a test environment. Once testing was complete and we were satisfied with the results the implementation into production began. The ESS application was installed on a Sun server running the Solaris 8 operating system. At the time, it was the only OS that allowed for encryption between the GUI clients and the ESS. Oracle 8 was chosen as the database type due to in-house expertise.

Once the ESS was installed, we defined 2 gateways for the initial 2 platforms that we were going to manage (Windows NT and RACF). Separate gateways are preferred because they can be shutdown independently of each other to minimize disruption (e.g. when troubleshooting or upgrades are performed).

The Control-SA Agents for Windows NT 4.0 and RACF were then installed. 3DES encryption was enabled for the communication between ESS and the agents. This ensures that passwords sent between the ESS and the agents are not transmitted in clear text over the network.
In order to reduce the number of privileged users in our environment, we configured the Control-SA Agent to execute the instructions received from ESS in the context of a generic user account (RSS Administrator) with sufficient privileges. For the Windows NT RSS, this user had to be a Domain Administrator. Although actions submitted from the ESS are recorded in the Windows NT security log as performed by the RSS Administrator, the ESS application maintains an audit log of the actions that an ESS Administrator has performed from the GUI. Therefore, using this generic account does not eliminate accountability. The ESS Administrator is a user that is allowed to sign-on to the Control-SA Windows GUI. To prevent misuse of the RSS Administrator account, we gave it a very strong password and configured ESS to automatically change the password for this account every 6 days. We also restricted logon access of

the RSS Administrator account to the Primary Domain Controller. This way the account cannot be utilized or exploited from a remote system.

Following the Control-SA Agents install, the Windows GUI was installed on the workstations that are used for security administration. In order to sign-on to the Control-SA GUI, one must have a valid ESS Administrator account and password. Having an ESS Administrator account does not give you any rights. In the ESS, Access Rules are created to give ESS Administrator (EA) accounts the right to perform actions such as password reset, revoke, restore, create, delete, modify, etc. Access Rules can be grouped and assigned to Security Groups (SG). Then EA can be connected to a SG instead of assigning access rules individually. The following Security Groups and access rights were created for our environment:

| | |
|---|---|
| Help Desk: | can perform password resets, account unlock, account revoke and account restore, view transaction logs. |
| System Admin: | can create/modify/delete users and groups, view transaction logs. |
| Auditors: | can view all entities including audit and transaction logs. |
| Operators | can stop/start gateways. |
| Desktop Support | can unlock accounts (no password reset). |
| Info Sec | can revoke (but not restore) accounts and view all entities for producing reports. |

By default, the ESS has one “superuser” EA that is all-powerful. Additional “superuser” EA accounts can be created if needed. To ensure accountability, the password for the default “superuser” account was sealed in an envelope and stored in a safe with strong physical access controls in place.
Only a “superuser” can change the password for an EA. Monthly reports are produced for the use of “superuser” accounts.

## Enterprise Users

To enable centralized administration, Control-SA uses the so-called Enterprise User (EU). A EU is only defined in the ESS application and it is used to connect all accounts (RSS Users) belonging to an employee from various platforms (see Figure 2 below).

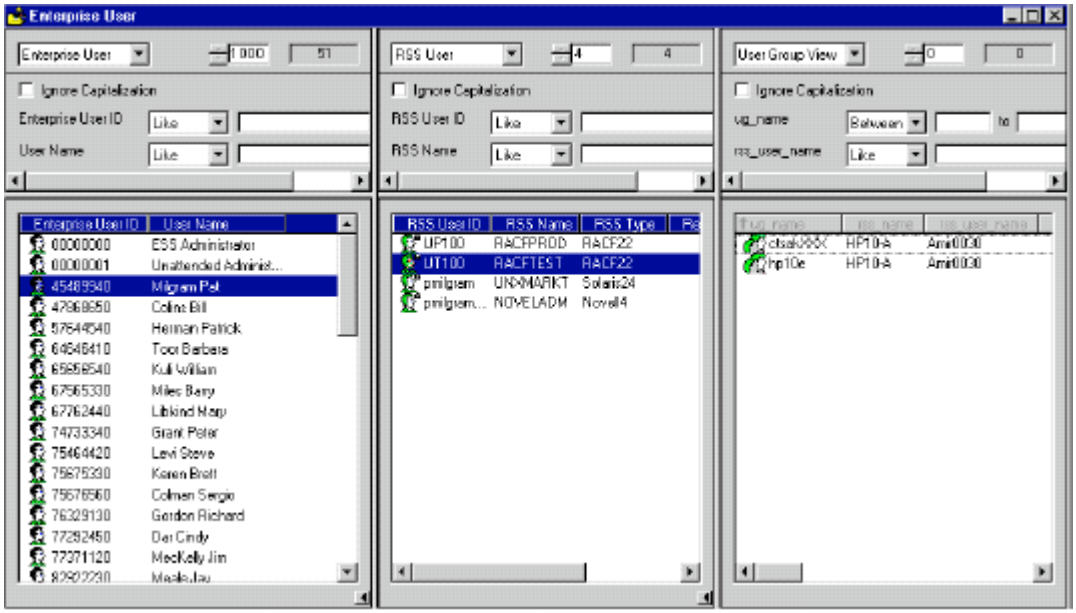


**Figure 2**[6]

As seen in figure 2 above, selecting the Enterprise User “Milgram Pat” in the left pane, the middle pane shows that this person has an “UP100” account on RACFPROD (production RACF), an “UT100” account on RACFTEST (test RACF), a “pmilgram” account on UNXMARKT server and NOVELADM server. The right-most pane shows which groups the “UT100” account belongs to.
This is very handy because changing the password for the EU will change the password for all connected RSS Users (on all managed platforms). The same applies for revoking and restoring a EU. Revoking a EU is an important part of the employee termination procedures to ensure all accounts belonging to the ex-employee are disabled in a timely fashion.
For our implementation it was decided that all RSS Accounts must be connected to a EU. This makes it very easy to produce a report displaying non-compliant RSS Accounts that could be an indication of a compromised system or abuse of privileges.
To create the EU we decided to export the Human Resources database to a flat file then import this file in Control-SA using a batch job that automatically creates the Enterprise Users. At this point all known employees from HR database had a EU created.
Next, the RSS Accounts from the managed systems were imported into ESS and the associations between the EU and RSS Accounts was performed.
This proved to be challenging due in part to years of decentralized administration and poor standards, which resulted in accounts being created with inconsistent naming conventions on each platform. E.g., one user could have “jdoe” as their user name in Windows NT and “jodoe” in RACF. The name (description field) for

[6] Enterprise SecurityStation User Guide (Windows GUI), Version 3.2.00, December 9, 2001, p 4-16

these accounts was also not entered exactly as in the HR database. We knew that matching these accounts with the EU would be a difficult task.
Not having the time and resources to modify all accounts (out of the scope of this project) we were forced to attempt a match based on the employee name and the account name. A Control-SA exit script was used to perform the automatic connection of RSS Users to a EU. Once the download was completed, we noticed that roughly 50% of the accounts matched to a EU. The rest of the RSS Ids had to be associated (connected) to a EU. This low rate of automatic connection was due to user accounts created inconsistently (as mentioned above).
Verification of all RSS User – EU connections had to be manually performed, which took a considerable amount of time. This was an important step because if an RSS User is connected to the wrong EU, the user may be granted excessive privileges or may get more access than it needs to perform its job. This would contravene the principle of "least privilege".
Now the organization was ready to use the tool for managing Windows NT and RACF user accounts and groups.

The next phase extended the Control-SA architecture to include another platform, which was Microsoft Exchange server. It made sense from a user provisioning perspective because all of our users have Exchange accounts. It also made sense from a security perspective when the employee termination process is considered.
The same steps were followed: installing the agent, establishing communication with ESS using 3DES encryption, downloading RSS Users from the Exchange server. The download action automatically connected the RSS Users to a EU with a success rate of approximately 50%. The rest of the RSS Ids had to be connected to EU manually. Again, a manual verification was performed.

## Templates

Control-SA allows the creation of templates for the RSS Users. Templates are invoked when a new RSS User is created. This speeds up considerably the user provisioning process because it fills-in the required fields (such as Name, Address, Country, Postal Code, Department, Budget Code, Phone Number, Fax, etc) with the information stored in the template or stored in another entity (such as EU). More than 70 templates were created, most of them for Exchange users, in order to accommodate our needs.
Template also ensures that RSS Users are created consistently across the enterprise.

## Job Codes

Control-SA allows the creation of Job Codes for increased user provisioning productivity. Job Codes are used to connect an RSS User to RSS Groups and can even be connected to Control-SA templates for automatically creating the

necessary RSS Users if they do not exist. Job Codes are important because they ensure user rights are assigned based on user's job role. If users relocate to another department, the EU for that particular user can simply be put in a different job code ensuring only the necessary rights are automatically granted (See Figure 3 below).

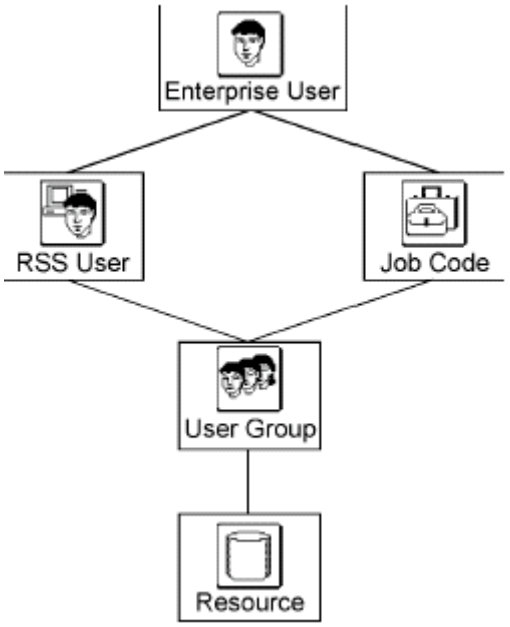


**Figure 3**[7]

Job Codes require careful planning before being deployed across the enterprise. At this time we don't have job codes created.

## Control-SA Passport

The final phase of this project will implement Control-SA Passport.
Control-SA Passport allows users to logon to a web site using their browser and manage their accounts. "Password reset relieves the management burden and costs of password-related support calls--while enforcing strong password policies--by enabling users to reset their own passwords and unlock their accounts without the aid of a help desk."[8]
The Control-SA Passport server was installed on a Windows 2000 server with IIS 5.0. The server was hardened per applicable Company standards.
The Passport application communicates with the ESS using the SSL protocol. On the ESS side, a superuser EA is required by Passport to perform account administration on behalf of the logged-on user. The application stores activity

[7] Enterprise SecurityStation User Guide (Windows GUI), Version 3.2.00, December 9, 2001, p 1-14.
[8] http://infosecuritymag.techtarget.com/2002/apr/cover_casestudy.shtml

logs in a Microsoft Access database located on the Passport server. These are separate from the IIS logs.
Control-SA Passport allows users to sign-on using a password specific for the Passport web site, or by using challenge/response (questions and answers) or both. The challenges can be site-defined or user-defined. The users cannot modify site-defined challenges (questions) but they can modify their answer to the challenge.
We decided to allow both logins via Passport password and site-defined challenges.
Due to privacy legislation we decided on a pool of 20 questions that do not refer to personal identifiable information such as Social Security Numbers, Social Insurance Numbers, Date of Birth, etc. Since we don't want people to be able to guess the answer, we decided to avoid questions based on publicly available information such as name, address, telephone number, etc. Once they sign-on to Passport using the initial password provided, the users are required change the initial password and to populate the answers for the 20 questions (challenges). Then users can sign-on using the Passport password or by correctly answering 5 out of 10 random questions from the pre-defined pool.
Repeated un-successful attempts (we set the threshold to 3 attempts) to sign-on results in the locking of the Passport account. At this point the user will have to call the Help Desk to unlock his/her Passport account and/or reset the password.
Although not fully implemented at this time, we ran a pilot for Control-SA Passport to determine the user feedback. The results were

- 84 % of the users would prefer to use Passport rather than contacting Help Desk.
- 32% of the users said Passport was very easy to use, 42% said Passport was easy to use and 26% said it was somewhat difficult to use.

Once Passport is extended to more platforms and applications, we are confident that the adoption of Passport will be even greater. This will contribute to the cost savings anticipated.
One question that surfaced when planning for the Passport implementation was: If the user cannot remember his/her network password and therefore can't logon to his/her workstation, how can he/she access the Passport web site? To solve this problem we decided to create a generic account (help) with a weak password that everyone can remember. One might quickly point out that this is a security risk. However, using Policy Editor we created a policy for this user so that when someone logs on using this account, Internet Explorer automatically starts and Passport web page is displayed. No other options, buttons or programs are available to this user profile and the account does not have access to any network resources. Surfing the Internet using this account is restricted at the proxy server. Therefore, this account can only be used to access the Passport web site.

## Password Synchronization

Another interesting feature of Control-SA is password synchronization. This allows users to maintain the same password across all systems. It is a well-known fact that if users are required to remember many passwords, they tend to pick passwords that are easy to remember or even worse, start to write them down if password complexity is enforced.
Password synchronization can help with this issue. If all the passwords are maintained in synch, the user has only one password to remember and stronger password policies could be enforced. The downside to password synchronization is the same as the downside of single sign-on: if a password were compromised, the attacker would have access to all the systems on which the user would have access.
If password synchronization is enabled, Control-SA can detect a password that was changed by the user and replicate that change across all managed platforms.
For this to work properly, the password policies on all systems have to be uniform.
Since we installed Control Agents for Windows NT, RACF and Microsoft Exchange, we could enable password synch between NT and RACF (not required for Microsoft Exchange since it integrates with Windows NT).
However, RACF has the following password limitations:

- Maximum password length: 8 characters.
- Passwords have to be alpha numeric. Includes the following signs: #, @, $.
- Passwords masking is supported. For example, the character in position 1 has to be alpha and character in position 2 has to be numeric, etc.
- Special characters are not supported.

On the Windows NT side, our account policy dictated that passwords must be minimum 8 characters long.
Due to the limitations of RACF password policies we decided not to implement password synch at this time.

## Current situation

Since we started with Control-SA implementation half a year ago, the following were accomplished:

- Installed Control-SA Agents for Windows NT 4.0, RACF (mainframe) and Microsoft Exchange Server.
- Conducted a Pilot for Control-SA Passport. Passport will soon be deployed to the entire company
- Currently preparing for the transition to Control-SA Agents for Windows 2003 with Active Directory and Microsoft Exchange 2000.
- We are evaluating the Control-SA Agents for Oracle, Entrust CA, LDAP and Unix. We plan to implement these agents in 2004.

- Once additional Control-SA agents are implemented we plan to activate the password synch feature (excluding mainframe).
- We reduced the number of privileged profiles. Previously everybody in the Help Desk and Desktop Support Group were part of the Account Operators group. Now there are no more users in the Account Operators group in the Windows NT domain and we reduced the number of Domain Administrators as well. Control-SA allowed us to delegate administration without elevating their privileges.
- We cleaned-up the environment of duplicate accounts, accounts that we no longer required, disabled accounts not used in a long time, etc.

Control-SA proved to be a very useful tool for user provisioning. The requests for new accounts, or modify or delete existing accounts can be completed by a single person on all platforms by using the appropriate template in a timely and efficient manner.

Information Security department can easily produce reports and take action on inactive accounts (such as accounts not used in 30 days), disabled accounts not used in 60 days, privileged accounts, accounts with no Enterprise User (possible rogue accounts) as well as monitor administrators delivering access rights (audit and transaction logs). Duplicate accounts are no longer created and we have a better access control mechanism in place.

With the implementation of additional agents in the future, as well as Control-SA Passport and password synch, we are looking to reduce further the time required for user provisioning as well as the volume of calls to Help Desk that are password related. Password synch will also help us implement a stronger and consistent password policy across the enterprise.

Job codes will be considered in the future; we'll start planning for them in 2004 after the migration to Windows 2003 and Active Directory.

## Conclusions

"Correctly implemented, identity management can deliver value by making it easier to do business with an organization." [9]
Identity Management allowed us to improve our reporting, auditing and access control mechanism that in turns ensures confidentiality, integrity, availability and accountability, as well as improve the user provisioning process thus saving time and money.
We believe that the advantages of centralized administration, enhanced security and improved user experience make Control-SA a valuable asset for the organization and we'll continue to build on this architecture.

[9] http://www.rsasecurity.com/solutions/idmgt/whitepapers/IDROI_WP_0403.pdf

## References

1. “RSA Security: Identity Management and Return on Investment - White Paper.” URL: http://www.rsasecurity.com/solutions/idmgt/whitepapers/IDROI_WP_0403.pdf (September 22, 2003)

2. “Liberty Alliance Project: Benefits of Federated Identity”. URL: http://www.projectliberty.org/resources/whitepapers/LAP%20Business%20Benefits%20White%20Paper%20v4.pdf (September 22, 2003)

3. Sudo Main Page. URL: http://www.courtesan.com/sudo/ (September 22, 2003)

4. “Business Layers: Identity Management.” URL: http://www.businesslayers.com/site/sol_identity.asp (September 22, 2003)

5. BMC Software, Inc. Enterprise SecurityStation User Guide (Windows GUI), Version 3.2.00, December 9, 2001, 1-3

6. BMC Software, Inc. Enterprise SecurityStation User Guide (Windows GUI), Version 3.2.00, December 9, 2001, 4-16

7. BMC Software, Inc. Enterprise SecurityStation User Guide (Windows GUI), Version 3.2.00, December 9, 2001, 1-14

8. Rutrell, Yassin. “What is Identity Management?” Tech Target. April 2002. URL: http://infosecuritymag.techtarget.com/2002/apr/cover_casestudy.shtml (September 22, 2003)

9. “RSA Security: Identity Management and Return on Investment - White Paper.” URL: http://www.rsasecurity.com/solutions/idmgt/whitepapers/IDROI_WP_0403.pdf (September 22, 2003)